KONINKRIJK DER NEDERLANDEN

Bureau voor de Industriële Eigendom

CERTIFIED COPY OF
PRIORITY DOCUMENT

Hierbij wordt verklaard, dat in Nederland op 13 juli 1999 onder nummer 1012581,

ten name van:

KONINKLIJKE KPN N.V.

te Groningen

een aanvrage om octrooi werd ingediend voor:

"Werkwijze voor het beschermen van een draagbare kaart",

en dat de hieraan gehechte stukken overeenstemmen met de oorspronkelijk ingediende stukken.

Rijswijk, 4 april 2000.

De Directeur van het Bureau voor de Industriële Eigendom,
voor deze,

A.W. van der Kruk.

Werkwijze voor het beschermen van een draagbare kaart

De uitvinding heeft betrekking op een werkwijze voor het beschermen van een draagbare kaart, die is voorzien van tenminste een crypto-algoritme voor vercijfering van data en/of authenticatie van de kaart, tegen het afleiden van de gebruikte geheime sleutel uit statistische analyse van zijn bij cryptografische bewerkingen naar buiten weglekkende informatie zoals stroomverbruikgegevens, electromagnetische straling en dergelijke, waarbij de kaart is voorzien van tenminste een schuifregister met een lineaire en een niet-lineaire terugkoppelfunctie voor het creëren van cryptografische algoritmen, waarbij de werkwijze omvat het laden van te verwerken data en een geheime sleutel in het schuifregister van de kaart.

Het gebruik van een geheime sleutel om invoerinformatie te verwerken en/of uitvoerinformatie voort te brengen is algemeen bekend bij cryptografische inrichtingen. Ook het gebruik van teruggekoppelde schuifregisters is algemeen bekend voor het creëren van cryptografische algoritmen.

Hierbij worden achtereenvolgens te verwerken data en een geheime sleutel in een of meer schuifregisters geladen. De volgorde van laden van data en sleutel is hierbij willekeurig. Vervolgens worden de uitvoer van het schuifregister en eventueel de inhoud van het schuifregister met behulp van lineaire en/of niet- lineaire terugkoppeling gebruikt om de uitvoer van het gehele algoritme te bepalen. De invoer van het schuifregister bestaat dan behalve uit de data en de sleutel ook uit een lineaire en/of niet-lineaire combinatie van de inhoud van het schuifregister.

Dergelijke schuifregisters worden algemeen toegepast bij draagbare kaarten zoals chipkaarten, telefoonkaarten, smart card producten en dergelijke.

Daar de geheime sleutel niet bekend is aan niet-bevoegde derden, kan men in beginsel uit de uitvoer van het algoritme noch de invoer noch de sleutel afleiden.

Er is nu echter gebleken, dat het bij chipkaarten en dergelijke mogelijk is om bij berekeningen de gebruikte geheime sleutel af te leiden uit een statistische analyse van het stroomverbruik van de kaart. Degelijke methoden zijn bekend onder de naam "Differential Power Analysis" (DPA) en worden beschreven in de Internet publicatie DPA Technical Information : "Introduction to Differential Power Analysis and Related Attacks" door P. Kocher et al , Cryptography Research, San Francisco, 1998.

Deze methoden zijn gebaseerd op het feit, dat in de praktijk bij cryptografische bewerkingen informatie weglekt naar buiten in de vorm van vermogensverbruiksgegevens, electromagnetische straling en dergelijke.

Zo vertonen logische microprocessoreenheden regelmatige transistorschakelpatronen, die uitwendig (d.w.z. buiten de microprocessor) waarneembaar elektrisch gedrag voortbrengen. Op deze wijze is het mogelijk om macro-karakteristieken zoals microprocessoractiviteit te identificeren door het registreren van het vermogensverbruik en informatie over de gebruikte geheime sleutel af te leiden via statistische analyse van de op deze wijze verkregen gegevens.

De uitvinding ondervangt nu dit bezwaar en voorziet in een draagbare kaart, die bestand is tegen dergelijke analyses en derhalve voorziet in een kaart, die gebruiksveilig is.

De werkwijze volgens de uitvinding wordt daartoe gekenmerkt, doordat men een algoritme op de kaart aanbrengt, dat zodanig geconstrueerd is, dat de verzameling van waarden van geregistreerde lekinformatiesignalen bestand is tegen het afleiden van de geheime sleutel via statistische analyse van deze waarden. Op voordelige wijze klokt men na het laden van de sleutel in het schuifregister vervolgens het schuifregister gedurende een bepaalde periode een aantal malen door, tenminste gebruikmakend van de lineaire terugkoppelfunctie.

Een geschikt alternatief volgens de uitvinding is het uitsluitend laden van de sleutel in het schuifregister bij een vaste inhoud van het schuifregister.

In een eerste voordelige uitvoeringsvorm van de uitvinding wordt eerst de sleutel geladen, vervolgens vindt het doorklokken plaats en daarna worden de data geladen.

In een andere voordelige uitvoeringsvorm van de uitvinding wordt eerst de sleutel geladen , vervolgens worden de data geladen in het schuifregister met uitsluitend gebruikmaking van de lineaire terugkoppelfunctie en vervolgens vindt het doorklokken plaats.

In nog een andere voordelige uitvoeringsvorm van de uitvinding worden eerst de data geladen, vervolgens wordt de sleutel geladen met uitsluitend gebruikmaking van de lineaire terugkoppelfunctie en daarna wordt doorgeklokt.

De uitvinding zal nu aan de hand van de tekening en de beschrijving in het volgende nader worden toegelicht bij wijze van niet-limitatief voorbeeld.

Fig. 1 toont schematisch een gebruikelijk schuifregister zoals dat wordt toegepast bij een draagbare kaart zoals een chipkaart en dergelijke.

Fig. 2 geeft schematisch een voordelige oplossing volgens de uitvinding weer, en

Fig. 3 geeft schematisch een andere voordelige oplossing volgens de uitvinding weer.

Onder verwijzing naar fig. 1 is een terugkoppelschuifregister 1, dat is aangebracht op iedere daartoe geschikte wijze op een ter wille van de eenvoud niet-weergegeven draagbare kaart zoals een chipkaart, telefoonkaart en dergelijke, met invoer 2 en uitvoer 3 getoond.

Het terugkoppelschuifregister 1 omvat een schuifregister 1a alsmede een terugkoppelfunctie, die in dit geval bestaat uit een lineaire functie 1b en een niet-lineaire functie 1c met een uitvoer 3a. Een dergelijk terugkoppelschuifregister komt vanwege zijn relatief lage kosten in aanmerking om te worden toegepast op bijvoorbeeld telefoonkaarten en dergelijke. Door de niet-lineaire functie kan ervoor worden gezorgd, dat elke bit afhankelijk is van elk aantal sleutelbits.

Schuifregisters zijn algemeen bekend en de werking ervan zal derhalve niet uitvoerig worden beschreven. Het schuifregister 1a bestaat uit een reeks bits. De lengte van een schuifregister wordt uitgedrukt in bits; bij een lengte van n bits spreekt men van een n-bit schuifregister. Telkens wanneer een bit nodig is, worden alle bits in het schuifregister 1 bit naar rechts geschoven. De nieuwe linker bit wordt berekend als functie van de andere bits in het register en de invoer.

De uitvoer van het schuifregister is 1 bit, dikwijls de minst significante bit. De periode van een schuifregister is de lengte van de uitvoerreeks alvorens de herhaling begint.

Data worden geladen via de invoer 2; de sleutel wordt geladen en via de uitvoer 3 of desgewenst 3a worden resultaten voortgebracht. Op een dergelijke situatie kan echter een aanval op de gebruikte geheime sleutel door middel van DPA worden uitgevoerd, gebaseerd op vermogensvariaties van het systeem bij berekeningen via statistische analyse van "lekgegevens"en foutencorrectietechnieken.

Hierbij wordt opgemerkt, dat het uit veiligheidsoverwegingen gewenst is om sleutel en data niet-lineair te laden in het schuifregister. Er is echter gebleken dat het op niet-lineaire wijze laden van sleutel en data in het schuifregister de kans op afleiden van de gebruikte geheime sleutel d.m.v. statistische analyse van het stroomverbruik bij berekeningen verhoogt.

In fig. 2 en fig. 3 geven dezelfde verwijzingscijfers als gebruikt in fig. 1 dezelfde onderdelen weer.

Fig. 2 toont nu een voordelige uitvoeringsvorm van de uitvinding, waarbij eerst de sleutel wordt geladen in het schuifregister, vervolgens data tenminste aanvankelijk uitsluitend met gebruikmaking van de lineaire terugkoppelfunctie worden geladen en vervolgens het

doorklokken (bijvoorbeeld 100 maal of meer) van het schuifregister plaatsvindt. Tijdens het laden van de data en desgewenst het daaropvolgende doorklokken wordt de niet-lineaire functie van het schuifregister geinactiveerd totdat het schuifregister in voldoende mate is doorgeklokt. Daarna wordt de niet-lineaire functie weer aangezet.

De lineaire terugkoppelfunctie 1b blijft hierbij aktief.

Het inactiveren resp. activeren van de niet-lineaire functie 1c kan op iedere daartoe geschikte wijze plaatsvinden, bijvoorbeeld met behulp van schakelaars.

Het schuifregister 1a wordt op voordelige wijze zodanig vaak doorgeklokt dat de inhoud van alle elementen van het schuifregister afhangt van een groot gedeelte van de bits van de sleutel.

In een andere voordelige uitvoeringsvorm wordt na het laden van de sleutel eerst doorgeklokt totdat de inhoud van alle elementen van het schuifregister afhangt van een groot gedeelte van de bits van de sleutel. Pas na dit doorklokken mogen data in het schuifregister 1a worden geladen en mogen ook niet-lineaire bewerkingen op de inhoud van het schuifregister plaatsvinden.

Het doorklokken vindt plaats op iedere aan deskundigen bekende wijze en zal derhalve niet nader worden toegelicht.

Opgemerkt wordt volledigheidshalve dat DPA slechts kan worden uitgevoerd indien er een niet-lineaire bewerking van de data met de sleutel plaatsvindt. Daar voorts de inspanning die voor DPA nodig is exponentieel stijgt met het aantal sleutelbits waar de bits in het schuifregister van afhangen, wordt op deze wijze bereikt, dat bij voldoende tussentijds doorklokken van het schuifregister 1a het toepassen van DPA niet snel tot succes leidt.

In fig. 3 is een voordelige variant van de uitvinding weergegeven, waarbij de sleutel bij vaste inhoud van het schuifregister (die ook uit louter nullen kan bestaan) is geladen en het doorklokken van het schuifregister plaatsvindt bij een actieve lineaire en een actieve niet-lineaire terugkoppelfunctie, maar zonder dat data worden geladen in het schuifregister gedurende de doorklokperiode. De invoer van data naar het schuifregister na het laden van de sleutel wordt hierbij losgekoppeld van het schuifregister en wordt weer hersteld na een bepaalde periode van doorklokken. Door de vaste inhoud van het schuifregister kunnen geen wijzigingen worden aangebracht en kan een niet-bevoegde derde geen verzameling van verschillende waarden van lekgegevens zoals het stroomverbruik vaststellen en onderwerpen aan statistische analyse teneinde de sleutel te achterhalen.

Bij deze oplossing volgens de uitvinding kan de sleutel derhalve op niet-lineaire wijze worden geladen en is het inactiveren van de niet-lineaire terugkoppelfunctie niet nodig.

In een andere voordelige uitvoeringsvorm van de uitvinding wordt in het geval dat de sleutel na het laden van data in het schuifregister niet bij een vaste inhoud van het schuifregister wordt geladen, de sleutel geladen in het schuifregister met slechts gebruikmaking van de lineaire terugkoppelfunctie, waarna vervolgens het doorklokken kan plaatsvinden.

Diverse modificaties van de werkwijze volgens de uitvinding zullen duidelijk zijn aan deskundigen na de bovenstaande beschrijving.

Dergelijk modificaties worden geacht binnen het kader van de uitvinding te vallen.

CONCLUSIES

1. Werkwijze voor het beschermen van een draagbare kaart, die is voorzien van tenminste een crypto-algoritme voor vercijfering van data en/of authenticatie van de kaart, tegen het afleiden van de gebruikte geheime sleutel uit statistische analyse van zijn bij cryptografische bewerkingen naar buiten weglekkende informatie zoals stroomverbruikgegevens, electromagnetische straling en dergelijke, waarbij de kaart is voorzien van tenminste een schuifregister met een lineaire en een niet-lineaire terugkoppelfunctie voor het creëren van cryptografische algoritmen, waarbij de werkwijze omvat het laden van te verwerken data en een geheime sleutel in het schuifregister van de kaart, met het kenmerk, dat men een algoritme op de kaart aanbrengt dat zodanig geconstrueerd is, dat de verzameling van waarden van geregistreerde lekinformatiesignalen bestand is tegen het afleiden van de geheime sleutel via statistische analyse van deze waarden.

2. Werkwijze volgens conclusie 1, met het kenmerk, dat men na het laden van de sleutel in het schuifregister vervolgens het schuifregister gedurende een bepaalde periode een aantal malen doorklokt, tenminste gebruikmakend van de lineaire terugkoppelfunctie.

3. Werkwijze volgens conclusie 2, met het kenmerk, dat men het schuifregister zolang doorklokt dat de inhoud van alle elementen van het schuifregister grotendeels afhankelijk is van de bits van de sleutel.

4. Werkwijze volgens conclusies 2 of 3 met het kenmerk dat men na het laden van de sleutel en het doorklokken vervolgens de data laadt in het schuifregister.

5. Werkwijze volgens een der conclusies 2 of 3 met het kenmerk dat men na het laden van de sleutel in het schuifregister de data laadt met uitsluitend gebruikmaking van de lineaire terugkoppelfunctie en vervolgens het schuifregister doorklokt.

6. Werkwijze volgens een der conclusies 2-5, met het kenmerk, dat het doorklokken van het schuifregister plaatsvindt bij een actieve lineaire terugkoppelfunctie en een niet-actieve niet-lineaire terugkoppelfunctie van het schuifregister.

7. Werkwijze volgens een der conclusies 2-6, met het kenmerk, dat het doorklokken van het schuifregister plaatsvindt bij een actieve lineaire en een actieve niet-lineaire terugkoppelfunctie van het schuifregister, waarbij echter geen data worden geladen in het schuifregister gedurende of vóór de doorklokperiode of vóór het laden van de sleutel.

8. Werkwijze volgens een der conclusies 5-7, met het kenmerk,dat men de niet-lineaire terugkoppelfunctie inactief maakt door de verbindingen ervan met het schuifregister alsmede desgewenst met de invoer te verbreken.

9. Werkwijze volgens een der conclusies 4-8, met het kenmerk, dat de invoer van data naar het schuifregister na het laden van de sleutel in het schuifregister wordt losgekoppeld van het schuifregister en weer wordt hersteld na de bovengenoemde bepaalde periode.

10. Werkwijze volgens een der voorgaande conclusies 1-9, met het kenmerk, dat men de sleutel uitsluitend laadt in het schuifregister bij een vaste inhoud van het schuifregister.

11. Werkwijze volgens een der voorgaande conclusies 1-9 met het kenmerk, dat indien de sleutel niet bij een vaste inhoud van het schuifregister wordt geladen, men de sleutel laadt in het schuifregister met slechts gebruikmaking van de lineaire terugkoppelfunctie, waarna het doorklokken plaatsvindt.

UITTREKSEL

Werkwijze voor het beschermen van een draagbare kaart, die is voorzien van tenminste een crypto-algoritme voor vercijfering van data en/of authenticatie van de kaart, tegen het afleiden van de gebruikte geheime sleutel uit statistische analyse van zijn bij cryptografische bewerkingen naar buiten weglekkende informatie zoals stroomverbruikgegevens, electromagnetische straling en dergelijk. De kaart is voorzien van tenminste een schuifregister met een lineaire en een niet-lineaire terugkoppelfunctie voor het creëren van cryptografische algoritmen. Men brengt een algoritme op de kaart aan, dat zodanig is geconstrueerd, dat de verzameling van waarden van geregistreerde lekinformatiesignalen bestand is tegen het afleiden van de geheime sleutel via statistische analyse van deze waarden.
Op voordelige wijze klokt men na het laden van de sleutel in het schuifregister het schuifregister door, tenminste gebruikmakend van de lineaire terugkoppelfunctie.
Een geschikt alternatief is het uitsluitend laden van de sleutel in het schuifregister bij een vaste inhoud van het schuifregister.

402571

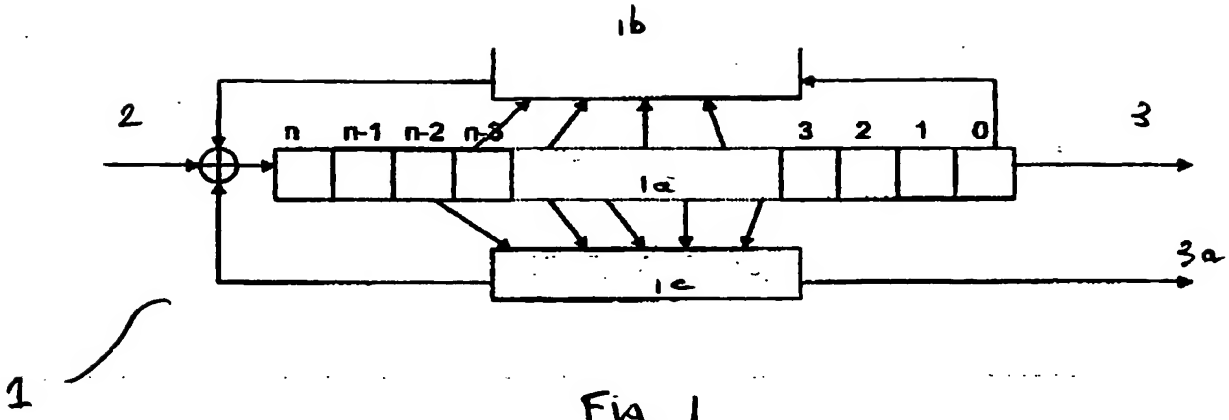

Fig. 1

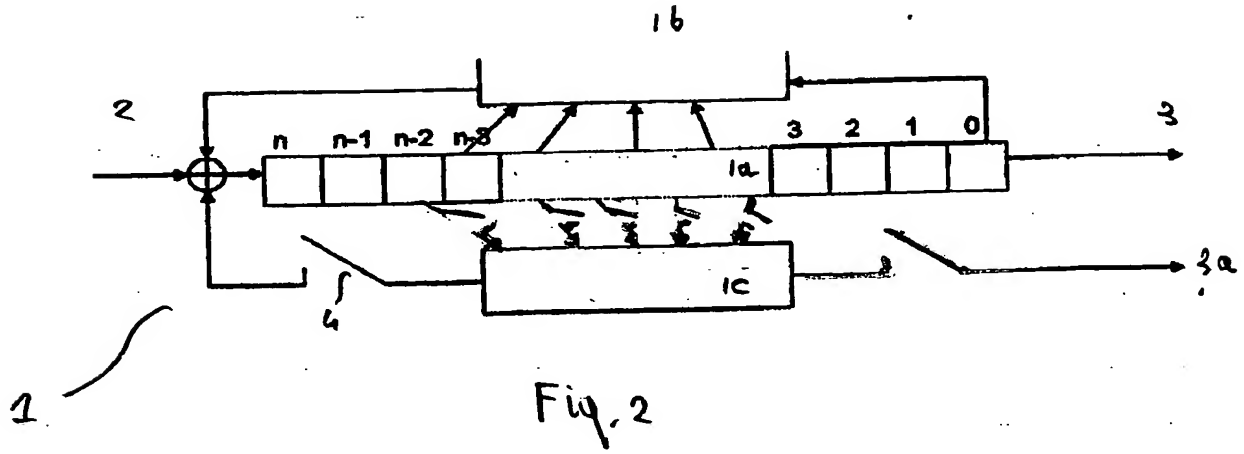

Fig. 2

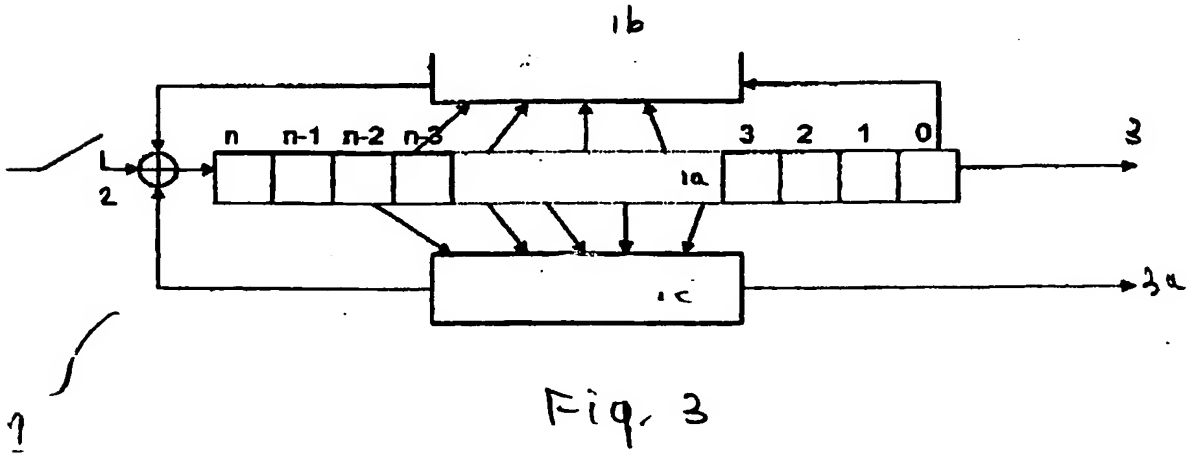

Fig. 3

KINGDOM OF T HE (crest) NETHERLANDS

PATENT OFFICE

This certifies that in the Netherlands on 13 July 1999 a patent application was filed under number 1012581, in the name of:

Koninklijke KPN N.V.

of Groningen

for: "A method for protecting a portable card"

and that the documents attached hereto are in accordance with the documents originally submitted.

Rijswijk, 4 April 2000

On behalf of the Chairman of the Patent Office,

(signature)

(A.W. van der Kruk)

ABSTRACT

A method for protecting a portable card, provided with at least a crypto algorithm for enciphering data and/or authenticating the card, against deriving the secret key used from statistical analysis of its information leaking away to the outside world in the event of cryptographic operations, such as power-consumption data, electromagnetic radiation and the like. The card is provided with at least a shift register having a linear and a non-linear feedback function for creating cryptographic algorithms. An algorithm is applied to the card, which is constructed in such a manner that the collection of values of recorded leak-information signals is resistant to deriving the secret key from statistical analysis of said values.

Advantageously, after the key has been loaded into the shift register, the shift register clocks on, using at least the linear-feedback function.

A suitable alternative is loading only the key into the shift register in the event of a fixed content of the shift register.2

A method for protecting a portable card.

The invention relates to a method for protecting a portable card, provided with at least a crypto algorithm for enciphering data and/or authenticating the card, against deriving the secret key used from statistical analysis of its information leaking away to the outside world in the event of cryptographic operations, such as power consumption data, electromagnetic radiation and the like, the card being provided with at least a shift register having a linear and a non-linear feedback function for creating cryptographic algorithms, the method comprising loading data to be processed and a secret key in the shift register of the card.

Using a secret key to process input information and/or to produce output information is generally known in the event of cryptographic devices. Using feedback shift registers is also generally known for creating cryptographic algorithms.

In this connection, data to be consecutively processed and a secret key are loaded into one or more shift registers. Here, the sequence of loading data and the key is random.

Subsequently, the output of the shift register and possibly the the shift-register contents are applied, using linear and/or non-linear-feedback, to determine the output of the entire algorithm. The input of the shift register then, apart from the data and the key, also consists of a linear and a non-linear combination of the shift-register contents.

Such shift registers are generally applied in the event of portable cards, such as chip cards, calling cards, smart-card products and the like.

Since the secret key is not known to unauthorised third parties, it is basically impossible to derive either the input or the key from the output of the algorithm.

Now it has become apparent, however, that for chip cards and the like it is possible, in the event of computations, to derive the secret key used from a statistical analysis of the power consumption of the card. Such methods are known as "Differential Power Analysis" (= DPA) and are described in the Internet publication DPA Technical Information: "Introduction to Differential Power Analysis and Related Attacks" by P. Kocher et al., Cryptography Research, San Francisco, 1998.

Said methods are based on the fact that, in practice, with cryptographic operations, information is leaking away to the outside world in the form of power-consumption data, electromagnetic radiation and the like.

Thus, logical microprocessor units show regular transistor-switching patterns which externally (i.e., outside the microprocessor) noticeably produce electrical behaviour.

In this manner, it is possible to identify macro characteristics, such as microprocessor activity, by recording the power consumption and deriving information on the secret key used by way of statistical analysis of the data thus obtained.

The invention now overcomes said drawback and provides a portable card which is resistant to such analyses and therefore provides a card which is safe to use.

The method according to the invention is characterised in that an algorithm is applied to the card which is constructed in such a manner that the collection of values of recorded leak-information signals is resistant to deriving the secret key by way of statistical analysis of said values. Advantageously, after loading the key into the shift register, the shift register is subsequently clocked on, during a specific period of time, several times, at least making use of the linear feedback function.

A suitable alternative according to the invention is loading only the key into the shift register in the event of a fixed content of the shift register.

In a first advantageous embodiment of the invention, there is first loaded the key, subsequently clocking on is performed, after which the data is loaded.

In another advantageous embodiment of the invention, the key is first loaded, subsequently the data is loaded into the shift register, making exclusive use of the linear feedback function and subsequently the clocking on is performed.

In yet another advantageous embodiment of the invention, the data is first loaded, subsequently the key is loaded, making exclusive use of the linear feedback function, whereafter clocking on is performed.

The invention will now be further explained with reference to the drawing and the description by way of non-limiting example.

FIG. 1 schematically shows a typical shift register as applied with a portable card, such as a chip card and the like.

FIG. 2 schematically shows an advantageous solution according to the invention, and

FIG. 3 schematically shows another advantageous solution according to the invention.

Referring now to FIG. 1, there is shown a feedback shift register 1, which is applied in any way suitable for that purpose to a portable card, not shown for simplicity's sake, such as a chip card, calling card and the like, having an input 2 and an output 3.

The feedback shift register 1 comprises a shift register 1a, as well as a feedback function, which in this case consists of a linear function 1b and a non-linear function 1c having an output 3a. Such a feedback shift register, due to its relatively low costs, is eligible for being applied to, e.g., calling cards and the like. The non-linear function may see to it that each bit depends on each number of key bits.

Shift registers are generally known and their operation will therefore not be described in detail. The shift register 1a consists of a series of bits. The length of a shift register is expressed in bits; in the event of a length of n bits, it is called an n-bit shift register.

Each time a bit is required, all bits in the shift register are shifted 1 bit to the right. The new left bit is calculated as a function of the bits remaining in the register and the input.

The output of the shift register is 1 bit, often the least significant bit. The period of a shift register is the length of the output series before repetition starts.

Data is loaded by way of the input 2; the key is loaded, and results are produced by way of the output 3 or, if so desired, 3a. In a similar situation, however, there may be carried out an attack on the secret key used by way of DPA, based on power variations of the system in the event of computations via statistical analysis of "leak data" and error-correcting techniques.

In this connection, it should be noted that, from a security viewpoint, it is desirable to load the key and the data non-linearly into the shift register. It has become apparent, however, that in the event of calculations, non-linearly loading the key and the data into the shift register increases the chance of deriving the secret key used through statistical analysis of the power consumption.

In FIG. 2 and FIG. 3, the same reference numerals as used in FIG. 1 refer to the same components.

FIG. 2 now shows an advantageous embodiment of the invention, the key first being loaded into the shift register, subsequently data being loaded, at least initially, exclusively using the linear-feedback function, and then the clocking on (e.g., 100 times or over) of the shift register taking place. During loading the data and, if so desired, the subsequent clocking on, the non-linear function of the shift register is deactivated until the shift register has been sufficiently clocked on. Then, the non-linear function is switched on once again.

In doing so, the linear-feedback function 1b continues to be active.

Deactivating and activating, as the case may be, the non-linear function 1c may take place in any way suitable for that purpose, e.g., using switches.

The shift register 1a is advantageously clocked on so many times that the content of all elements of the shift register depends on a large portion of the bits of the key.

In another advantageous embodiment, after loading the key there is first clocked on until the content of all elements of the shift register depends on a large portion of the bits of the key. Only after said clocking on, the data in the shift register 1a is permitted to be loaded and non-linear operations on the content of the shift register are also permitted to be effected.

Clocking on takes place in any way known to those skilled in the art and will therefore not be explained in further detail.

For completeness' sake, it should be noted that DPA is only capable of being carried out if there takes place a non-linear operation of the data with the key. Since, in addition, the effort required for DPA rises exponentially with the number of key bits on which the bits in the shift register depend, it is achieved in this manner that, in the event of sufficient interim clocking on of the shift register 1a, applying DPA does not result in short-term success.

In FIG. 3, there is shown an advantageous variant of the invention, the key having been loaded with a fixed content of the shift register (which may also consist purely of zeros) and clocking on the shift register taking place with an active linear and an active non-linear feedback function, but without data being loaded into the shift register during the clocking-on period. In doing so, the input of data into the shift register after loading the key is disconnected from the shift register and is reinstated again after a

specific clocking-on period. Due to the fixed content of the shift register, it is not permitted to apply any modifications and an unauthorised third party shall not be capable of determining a collection of different values of leak data, such as power consumption, and subject it to statistical analysis in order to retrieve the key.

In this solution according to the invention, the key may therefore be loaded non-linearly, and deactivating the non-linear feedback function will not be required.

In another advantageous embodiment of the invention, in the event that the key, after data has been loaded into the shift register, is not loaded with the fixed content of the shift register, the key is loaded into the shift register using only the linear-feedback function, whereafter subsequent clocking on is permitted to take place.

After the aforementioned description, various modifications of the method according to the invention will become apparent to those skilled in the art.

Such modifications shall be deemed to fall within the scope of the invention.

CLAIMS

1. A method for protecting a portable card provided with at least a crypto algorithm for enciphering data and/or authenticating the card against deriving the secret key used from statistical analysis of its information leaking away to the outside world in the event of cryptographic operations, such as power-consumption data, electromagnetic radiation and the like, the card being provided with at least a shift register having a linear and a non-linear feedback function for creating cryptographic algorithms, the method comprising loading data to be processed and a secret key in the shift register of the card, characterised in that an algorithm is applied to the card which is constructed in such a manner that the collection of values of recorded leak-information signals is resistant to deriving the secret key by way of statistical analysis of said values.

2. The method according to claim 1, characterised in that, after the key has been loaded into the shift register, the shift register subsequently, during a specific period, clocks on several times, at least using the linear-feedback function.

3. The method according to claim 2, characterised in that the shift register is clocked on for so long that the content of all elements of the shift register largely depend on the bits of the key.

4. The method according to claim 2 or 3, characterised in that, after the key has been loaded and after clocking on, the data is subsequently loaded into the shift register.

5. The method according to either of the claims 2 and 3, characterised in that after the key has been loaded into the shift register, the data is loaded using only the linear-feedback function and the shift register subsequently clocks on.

6. The method according to any one of claims 2 to 5, characterised in that clocking on the shift register takes place with an active linear-feedback function and a non-active, non-linear feedback function of the shift register.

7. The method according to any one of claims 2 to 6, characterised in that clocking on the shift register takes place with an active linear and an active non-linear feedback function of the shift register, no data being loaded into the shift register, however, during, or prior to, the clocking-on period or prior to loading the key.

8. The method according to any one of claims 5 to 7, characterised in that the non-linear feedback function is deactivated by disconnecting the connections thereof with the shift register as well as, if so desired, with the input.

9. The method according to any one of the claims 4 to 8, characterised in that the input of data into the shift register after loading the key into the shift register is disconnected from the shift register and is reinstated after the aforementioned specific period.

10. The method according to any one of the preceding claims 1 to 9, characterised in that the key is only loaded into the shift register in the event of a fixed content of the shift register.

11. The method according to any one of the preceding claims 1 to 9, characterised in that, if the key is not loaded with a fixed content of the shift register, the key is loaded into the shift register using only the linear-feedback function, whereafter clocking on takes place.

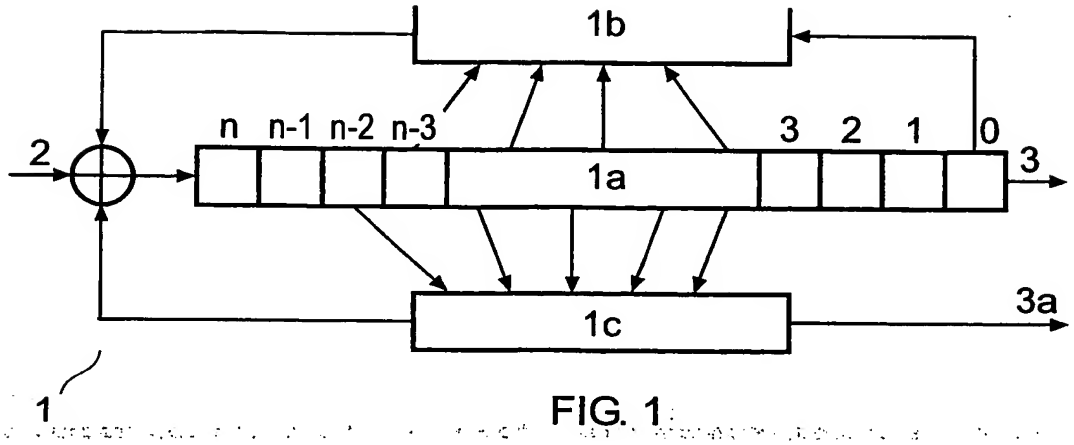

FIG. 1

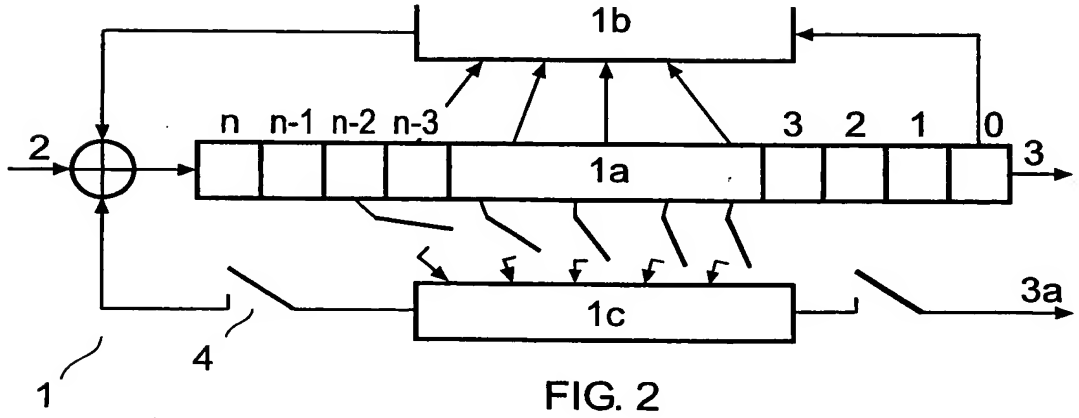

FIG. 2

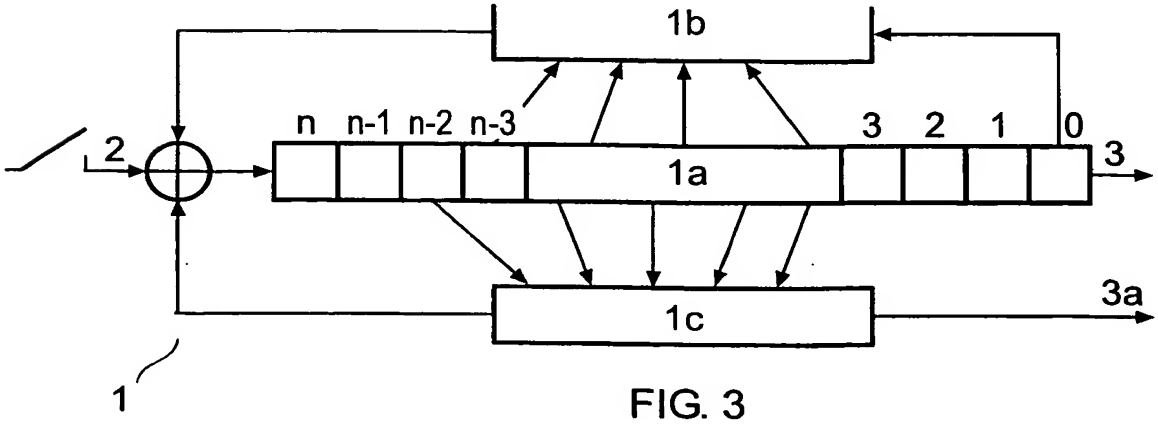

FIG. 3